API Authorization Management

CC by 4.0

What is API Authorization?

Process of controlling access to APIs based on the identity and permissions of the requesting user or application.

Why securing APIs matter?

- Protect sensitive data
- Preventing unauthorized access
- Ensure compliance with security standards and regulations

Key Concepts

Key Concepts

API resources:

Represent the endpoints or functionalities exposed by an API.

Scopes:

Known as permissions. Scopes represent an action an application can perform on behalf of a user.

Types of API Authorization

- Role-Based Access Control (RBAC)
- Attribute-Based Access Control (ABAC)

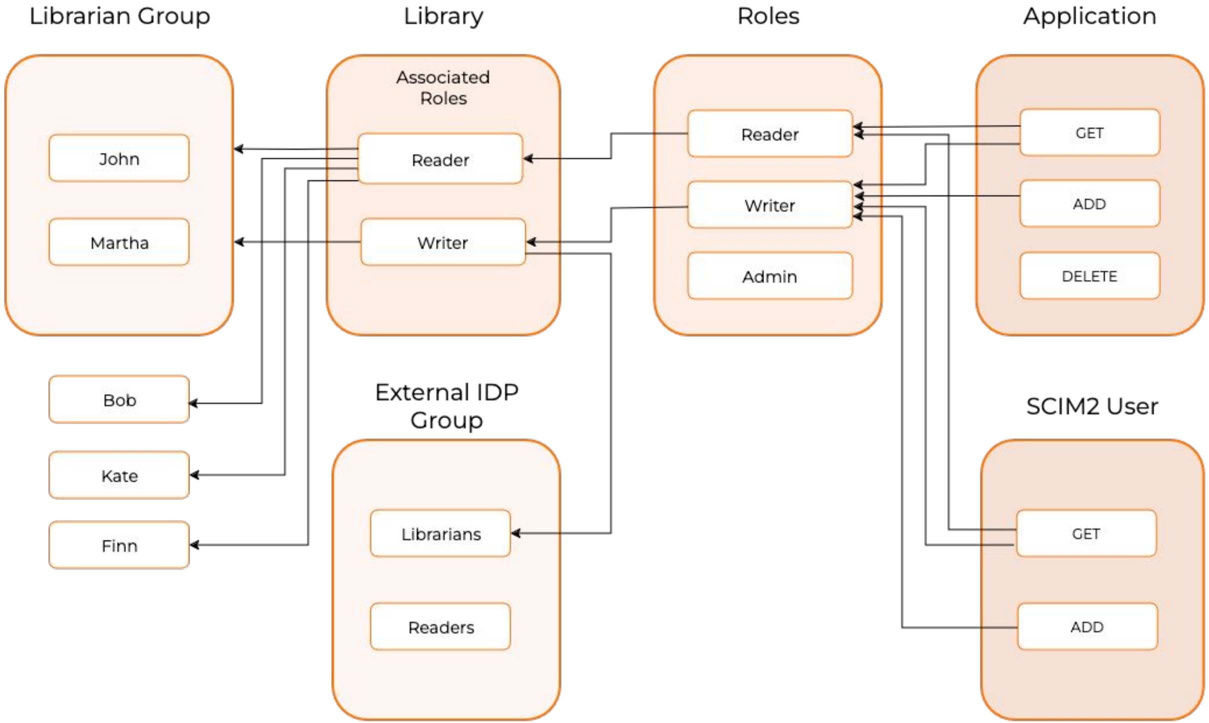
RBAC for API resources

Role Based Access Control (RBAC)

An access control model where access to resources is based on the roles assigned to users or applications.

- Implement granular access control to specific API endpoints or functionalities.
- Users or applications assigned roles based on their job responsibilities or required permissions.
- Only users or applications with appropriate roles can access.

How it works?


Librarian Group
John
Martha
Bob
Kate
Finn
Library
Associated Roles
Reader
Writer
External IDP Group
Librarians
Readers
Roles
Reader
Writer
Admin
Application
GET
ADD
DELETE
SCIM2 User
GET
ADD

Quick Recap

What you learnt

1. Overview of API authorization
2. Benefits of securing APIs
3. Types of API authorization
4. Role Based Access Control (RBAC)

Any Questions ?

Reach us through the following channels

✉ iam-dev@wso2.org

https://stackoverflow.com/questions/tagged/wso2-identity-server

https://discord.com/invite/Xa5VubmThw

Thanks!

wso2.com